CLAIM AMENDMENTS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims

1. (Currently Amended) A data processing system, comprising:

a first integrated circuit, the first integrated circuit ~~including~~ comprising:

a first logic block ~~configured to generate~~ generating a data stream;

a hardware encryption circuit coupled to the first logic block, ~~and configured to encrypt~~ the hardware encryption circuit encrypting the data stream to generate an encrypted data stream; and

a first Peripheral Component Interconnect Express (PCI-Express) - compatible interface circuit ~~configured to support~~ supporting data communication over a plurality of PCI-Express virtual channels, wherein the plurality of PCI-Express virtual channels ~~includes~~ comprises at least an unencrypted default virtual channel and a dedicated encrypted virtual channel, ~~that is incapable of being bypassed or disabled, and is configured to communicate encrypted data exclusively,~~ wherein the first PCI-Express-compatible interface circuit includes a first plurality of channel interconnects, each channel interconnect associated with a virtual channel among the plurality of virtual channels, wherein a first channel interconnect among the plurality of virtual channels is coupled to the hardware encryption circuit to

receive the encrypted data stream, and wherein the first PCI-Express-compatible interface circuit ~~is configured to communicate~~ communicates the encrypted data stream from the hardware encryption circuit over the dedicated encrypted virtual channel;

a second integrated circuit coupled to the first integrated circuit by a PCI-Express-compatible interconnect, the second integrated circuit ~~including~~ comprising:

a second PCI-Express-compatible interface circuit coupled to the PCI-Express-compatible interconnect to receive the encrypted data stream over the dedicated encrypted virtual channel, the second PCI-Express-compatible interface circuit ~~including~~ comprising:

a second plurality of channel interconnects, each channel interconnect associated with a virtual channel among the plurality of virtual channels;

a hardware decryption circuit coupled to a first channel interconnect among the second plurality of channel interconnects for the second PCI-Express-compatible interface circuit and configured to decrypt the encrypted data stream; and

a second logic block coupled to the hardware decryption circuit and configured to use the decrypted data stream; and

control logic coupled to at least one of the first and second PCI-Express-compatible interface circuits and configured to communicate authorization data over the default virtual channel to authorize secure communication between the first and second integrated circuits over the dedicated encrypted virtual channel, wherein all data sent over the dedicated encrypted virtual channel are encrypted, and access control and decoding are separately performed on the first and second integrated circuits for the dedicated encrypted virtual channel.

2. (Currently Amended) A circuit arrangement, comprising:

a multi-channel serial interface circuit configured to communicate data over a serial interconnect using a plurality of virtual channels; and

a hardware encryption circuit coupled to the multi-channel serial interface circuit and configured to encrypt all data communicated over a dedicated encrypted virtual channel~~, that is incapable of being bypassed or disabled,~~ among the plurality of virtual channels,

wherein all data sent over the dedicated encrypted virtual channel are encrypted, and access control and decoding are separately performed on two integrated circuits for the dedicated encrypted virtual channel.

3. (Previously Presented) The circuit arrangement of claim 2, the multi-channel serial interface circuit further comprising:

PCI-Express-compatible interface logic coupled to the hardware encryption circuit and configured to communicate encrypted data output by the hardware encryption circuit over a PCI-Express-compatible interconnect.

4. (Previously Presented) The circuit arrangement of claim 2, further comprising:

a logic block coupled to the hardware encryption circuit and configured to output data for communication over the serial interconnect to the hardware encryption circuit such that the data output by the logic block is encrypted prior to communication over the serial interconnect.

5. (Original) The circuit arrangement of claim 4, wherein the logic block is additionally configured to output additional data for communication over an unencrypted virtual channel among the plurality of virtual channels.

6. (Original) The circuit arrangement of claim 4, wherein the logic block is configured to output data over the serial interconnect solely over the dedicated encrypted virtual channel.

7. (Previously Presented) The circuit arrangement of claim 4, further comprising:

a second logic block coupled to the multi-channel serial interface circuit and configured to output data for communication over an unencrypted virtual channel among the plurality of virtual channels.

8. (Previously Presented) The circuit arrangement of claim 4, further comprising:

a second logic block coupled to the hardware encryption circuit and configured to output data for communication over the dedicated encrypted virtual channel.

9. (Previously Presented) The circuit arrangement of claim 4, further comprising:

a hardware decryption circuit coupled intermediate the multi-channel serial interface circuit and the logic block, the hardware decryption circuit configured to decrypt encrypted data received from the serial interconnect by the multi-channel serial interface circuit and communicated over the dedicated encrypted virtual channel.

10. (Original) The circuit arrangement of claim 4, wherein the plurality of virtual channels includes a default virtual channel configured to communicate

authorization data for authorizing secure communication over the dedicated encrypted virtual channel.

11. (Previously Presented) An integrated circuit comprising:

the multi-channel serial interface circuit and hardware encryption circuit of claim 2.

12. (Previously Presented) A data processing system, comprising:

the integrated circuit of claim 11, and

a second integrated circuit comprising:

a second multi-channel serial interface circuit configured to receive the encrypted data communicated over the serial interconnect by the first multi-channel serial interface circuit, and

a hardware decryption circuit configured to decrypt the encrypted data received over the serial interconnect.

13. (Canceled)

14. (Currently Amended) A circuit arrangement, comprising:

a multi-channel serial interface circuit configured to communicate data over a serial interconnect using a plurality of virtual channels; and

a hardware decryption circuit coupled to the multi-channel serial interface circuit and configured to decrypt all data received from the serial interconnect by the multi-channel serial interface that has been communicated over the serial interconnect on a dedicated encrypted virtual channel, ~~that is incapable of being bypassed or disabled,~~ among the plurality of virtual channels, wherein all data sent over the dedicated encrypted virtual channel are encrypted and access control, and decoding are performed on two separate integrated circuits for the dedicated encrypted virtual channel.

15. (Currently Amended) A method of communicating data over a serial interconnect, the method comprising:

encrypting a data stream using a hardware encryption circuit disposed on ~~an~~ a first integrated circuit; and

communicating the encrypted data stream over a serial interconnect using a multi-channel serial interface circuit disposed on the first integrated circuit, wherein communicating the encrypted data stream includes communicating the encrypted data stream over a dedicated encrypted virtual channel, ~~that is incapable of being bypassed or disabled,~~ from among a plurality of virtual channels supported by the multi-channel serial interface circuit, ~~and~~ wherein the dedicated encrypted virtual channel is dedicated to the communication of encrypted data, and wherein all data sent over the dedicated encrypted virtual channel are encrypted, and access

control and decoding are separately performed on two integrated circuits for the dedicated encrypted virtual channel.

16. (Currently Amended) The method of claim 15, further comprising:

communicating the encrypted data over a PCI-Express-compatible interconnect, wherein the multi-channel serial interface circuit comprises PCI-Express-compatible interface logic coupled to the hardware encryption circuit~~, and wherein communicating the encrypted data stream over the serial interconnect comprises communicating the encrypted data over a PCI-Express compatible interconnect~~.

17. (Previously Presented) The method of claim 15, further comprising:

generating the data stream from a logic block disposed on the integrated circuit.

18. (Currently Amended) The method of claim 17, further comprising:

configuring ~~wherein~~ the logic block ~~is configured~~ to output data over the serial interconnect solely over the encrypted virtual channel.

19. (Previously Presented) The method of claim 17, further comprising:

generating a second data stream from a second logic block disposed on the integrated circuit, and

communicating the second data stream over the serial interconnect using an unencrypted virtual channel among the plurality of virtual channels supported by the multi-channel serial interface circuit.

20. (Original) The method of claim 17, further comprising:

decrypting a second encrypted data stream received from the serial interconnect by the multi-channel serial interface circuit and communicated over the dedicated encrypted virtual channel using a hardware decryption circuit disposed on the integrated circuit; and

communicating the decrypted data stream to the logic block.

21. (Previously Presented) The method of claim 17, wherein the plurality of virtual channels includes a default virtual channel, the method further comprising:

communicating authorization data over the default virtual channel to authorize secure communication over the dedicated encrypted virtual channel.

22. (Original) The method of claim 17, further comprising:

receiving the encrypted data stream from the serial interconnect using a second multi-channel serial interface circuit disposed on a second integrated circuit; and

decrypting the encrypted data stream using a hardware decryption circuit disposed on the second integrated circuit.

23. (Currently Amended) A method of providing access control for a digital data stream, the method comprising:

decrypting a first encrypted data stream in a first integrated circuit to generate a first decrypted data stream;

re-encrypting the first decrypted data stream in the first integrated circuit to generate a second encrypted data stream;

communicating the second encrypted data stream from the first integrated circuit to a second integrated circuit over a multi-channel serial interconnect to which the first and second integrated circuits are connected by communicating the second encrypted data stream over a dedicated encrypted virtual channel, ~~that is incapable of being bypassed or disabled,~~ among a plurality of virtual channels supported by the multi-channel serial interconnect, wherein all data sent over the dedicated encrypted virtual channel are encrypted and access control, and decoding are performed separately on the first and second integrated circuits for the dedicated encrypted virtual channel; and

decrypting the second encrypted data stream in the second integrated circuit to generate a second decrypted data stream.

24. (Previously Presented) The method of claim 23, further comprising:

demodulating a modulated input signal to generate the first encrypted data stream.

25. (Previously Presented) The method of claim 24, further comprising:

decoding the second decrypted data stream in the second integrated circuit to generate a decoded data stream.

26. (Currently Amended) The method of claim 24, further comprising:

performing MPEG decoding on the second decrypted data stream, wherein the modulated input signal comprises a satellite broadcast signal, and wherein the first encrypted data stream comprises an encrypted MPEG data stream~~, and wherein decoding the second decrypted data stream in the second integrated circuit comprises performing MPEG decoding on the second decrypted data stream~~.

27. (Currently Amended) The method of claim 23, further comprising:

~~wherein decrypting the first encrypted data stream includes~~

performing regional access control on the first encrypted data stream.

28. (Currently Amended) The method of claim 23, further comprising: ~~wherein decrypting the first encrypted data stream includes~~ performing subscriber access control on the first encrypted data stream.

29. (Currently Amended) The method of claim 23, further comprising: ~~wherein~~ disposing the first and second integrated circuits ~~are disposed~~ in a set top box.

30. (Currently Amended) The method of claim 23, further comprising: ~~wherein~~ disposing the first integrated circuit ~~is disposed~~ on an access card coupled to the second integrated circuit via a connector.

31. (Currently Amended) The method of claim 23, further comprising: ~~wherein~~ performing ~~re-encrypting~~ re-encryption of the first decrypted data stream ~~is performed by~~ with hardware encryption logic disposed on the first integrated circuit.

32. (Currently Amended) A circuit arrangement, comprising:

first decryption logic configured to perform access control and to decrypt a first encrypted data stream and generate ~~therefrom~~ a first decrypted data stream, the first decryption logic disposed on a first integrated circuit in a processor chip set;

encryption logic configured to re-encrypt the first decrypted data stream and generate therefrom a second encrypted data stream;

decoder logic on a second integrated circuit in the processor chip set; and

a multi-channel serial interface circuit configured to communicate the second encrypted data stream over a multi-channel serial interconnect by communicating the second encrypted data stream over a dedicated encrypted virtual channel, ~~that is incapable of being bypassed or disabled,~~ among a plurality of virtual channels supported by the multi-channel serial interconnect, wherein all data sent over the dedicated encrypted virtual channel are encrypted and access control, and decoding are performed separately on the first and second integrated circuits for the dedicated encrypted virtual channel.

33. (Currently Amended) The circuit arrangement of claim 32, further comprising:

second decryption logic ~~configured to decrypt~~ decrypting the second encrypted data stream and generating ~~generate therefrom~~ a second decrypted data stream.

34. (Currently Amended) The circuit arrangement of claim 33, further comprising:

demodulation logic ~~configured to generate~~ generating the first encrypted data stream from a modulated input signal.

35. (Currently Amended) The circuit arrangement of claim 34, ~~further comprising:~~wherein the decoder logic ~~configured to decode~~ decodes the second decrypted data stream.

36. (Original) The circuit arrangement of claim 35, wherein the modulated input signal comprises a satellite broadcast signal, wherein the first encrypted data stream comprises an encrypted MPEG data stream, and wherein decoding the second decrypted data stream in the second integrated circuit comprises performing MPEG decoding on the second decrypted data stream.

37. (Currently Amended) The circuit arrangement of claim 35, wherein the demodulation logic, ~~the first decryption logic,~~ the encryption logic, and the multi-channel serial interface circuit are disposed on ~~a~~ the first integrated circuit, wherein the second decryption logic ~~and decoder logic are~~ is disposed on ~~a~~ the second integrated circuit, and wherein the second integrated circuit includes a

second multi-channel serial interface circuit coupled to the multi-channel serial interconnect to receive the second encrypted data stream ~~therefrom~~.

38. (Currently Amended) The circuit arrangement of claim 32, wherein the first decryption logic ~~is configured to perform~~ performs regional access control on the first encrypted data stream.

39. (Currently Amended) The circuit arrangement of claim 32, wherein the first decryption logic ~~is configured to perform~~ performs subscriber access control on the first encrypted data stream.

40. (Currently Amended) The circuit arrangement of claim 32, wherein the multi-channel serial interface circuit comprises PCI-Express-compatible interface logic coupled to the encryption logic, ~~and configured to communicate~~ communicating the first encrypted data stream over a PCI-Express-compatible interconnect.

41-45. (Canceled)